

## UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA )

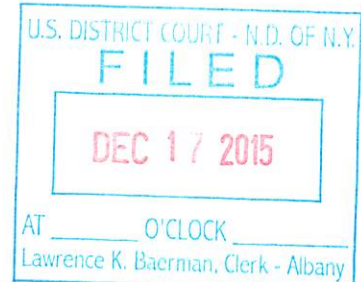
v. )

EDWARD WERNER, )

Defendant(s) )

Case No. 15-MJ-486 CFH

## CRIMINAL COMPLAINT



I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 23, 2015 through and including March 3, 2015 in the county of Schoharie in the Northern District of New York the defendant(s) violated:

*Code Section*

18 U.S.C. § 2252A(a)(2) and (b)(1)

*Offense Description*

Receipt and Attempted receipt of child pornography

This criminal complaint is based on these facts:  
Click here to enter text.

☒ Continued on the attached sheet.

A handwritten signature in blue ink, appearing to read "David C. Fallon".

*Complainant's signature*DAVID C. FALLON, SA FBI*Printed name and title*

Sworn to before me and signed in my presence.

Date: December 17, 2015

A handwritten signature in blue ink, appearing to read "Christian F. Hummel".

*Judge's signature*City and State: Albany, New YorkHon. Christian F. Hummel, U.S. Magistrate Judge*Printed name and title*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF NEW YORK**

**AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT**

I, David C. Fallon, being duly sworn, depose and state:

**I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since May 1991. As such, I am an investigative or law enforcement officer of the United States within the meaning of Title 18 United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1). I have been a law enforcement officer for twenty-four years.

2. This affidavit is made in support of an application for a criminal complaint charging Edward Werner with violations of Title 18, United States Code, § 2252A(a)(2) and (b)(1) (attempted receipt and possession of child pornography).

3. Because this affidavit is being submitted for the limited purpose of securing a criminal Complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that Edward Werner has committed violations of 18 U.S.C. § 2252A(a)(2) and (b)(1).

**II. THE INVESTIGATION**

**“Website A” and “The Network”**

4. On or about February 20, 2015, a computer server hosting “Website A”<sup>1</sup> was

---

<sup>1</sup> The actual name of “Website A” is known to law enforcement. Disclosure of the name of the site would

seized from a web-hosting facility in Lenoir, North Carolina. “Website A” was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time “Website A” ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of “Website A.” Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of “Website A,” which are described below.

5. “Website A” operated on a network (“the Network”<sup>2</sup>) available to Internet users who are aware of its existence. “The Network” is designed specifically to facilitate anonymous communication over the Internet. In order to access “the Network”, a user must install computer software that is publicly available, either by downloading software to the user’s existing web browser, downloading free software available from “the

---

potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as “Website A.”

2 The actual name of “the Network” is known to law enforcement. “The Network” remains active and disclosure of the name of “the Network” would potentially alert its members to the fact that law enforcement action is being taken against “the Network”, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as “the Network.”

Network's" administrators, or downloading a publicly-available third-party application.<sup>3</sup> Websites that are accessible only to users within "the Network" can be set up within "the Network" and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.<sup>4</sup> Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to "the Network", however, a user had to know the exact web address of "Website A" in order to access it. Websites on "the Network" are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

6. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The

---

3 Users may also access "the Network" through so-called "gateways" on the open Internet; however, use of those gateways does not provide users with the full anonymizing benefits of "the Network".

4 Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

7. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

8. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

9. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors; the abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit conduct); and “scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

10. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The “last post” section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images,

thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

11. A review of the various topics within the “[Website A] information and rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

12. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. In total, “Website A” contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

13. “Website A” also included a feature referred to as “[Website A] Image Hosting.” This feature of “Website A” allowed users of “Website A” to upload links to images of child pornography that are accessible to all registered users of “Website A.” On February 12, 2015, an FBI Agent accessed a post on “Website A” titled “Giselita” which was created by a particular “Website A” user. The post contained links to images stored on “[Website A] Image Hosting.” The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.



Court-Authorized Use of Network Investigative Technique

14. On February 20, 2015, the same date “Website A” was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique (“NIT”) on “Website A” in an attempt to identify the actual IP addresses and other identifying information of computers used to access “Website A.” Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into “Website A” by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user’s computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing “Website A.” That data included: the computer’s actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer’s Host Name; the computer’s active operating system username; and the computer’s MAC address.

“cunnylicker” on “Website A”

15. According to data obtained from logs on “Website A,” monitoring by law enforcement and the deployment of a NIT, a user with the user name “cunnylicker”



engaged in the following activity on “Website A.”

16. The profile page of user “cunnylicker” indicated this user originally registered an account on “Website A” on January 26, 2015. Profile information on “Website A” may include contact information and other information that is supplied by the user. It also contains information about that user’s participation on the site, including statistical information about the user’s posts to the site and a categorization of those posts. According to the user “cunnylicker’s” profile, this user was a Newbie Member of “Website A.” Further, according to the Statistics section of this user’s profile, the user “cunnylicker” had been actively logged into the website for a total of 9 hours, 24 minutes and 4 seconds, between the dates of January 26, 2015 and March 03, 2015.

IP Address and Identification of User “cunnylicker” on “Website A”

17. According to data obtained from logs on “Website A,” monitoring by law enforcement, and the deployment of a NIT, on February 23, 2015 at 21:21 UTC, the user “cunnylicker” engaged in the following activity on “Website A” from IP address 72.10.204.74. During the session described below, this user browsed “Website A” after logging into “Website A” with a username and a password.

18. On February 23, 2015 at 21:21 UTC, the user “cunnylicker” with IP address 72.10.204.74 accessed the post entitled “Gabby Full Video Collection” which was located in the “Pre-teen Videos,” “Girls HC (hardcore)” section of “Website A.” Among other things, this post contained a link to a video that purported to depict a prepubescent female engaged in hardcore sexual activity.

19. During the following additional sessions, the user “cunnylicker” also browsed “Website A” after logging into “Website A” with a username and password. During

these sessions, the user's IP address information was not collected.

20. On March 3, 2015, the user "cunnylicker" accessed a post that contained an embedded set of 16 images depicting a prepubescent female performing oral sex upon the penis of an adult male.

21. Also on March 3, 2015, the user "cunnylicker" accessed a post containing a set of embedded images in which the majority of the images focused on the exposed genitals of a nude prepubescent female. The female's genitals are covered in a substance which appears to be semen. In some of the images, a finger of an adult male is touching the female's genitals.

22. Using publicly available websites, FBI Special Agents were able to determine that the above IP Address was operated by the Internet Service Provider ("ISP") "Midtel.net."

23. In June 2015, an administrative subpoena/summons was served to Midtel.net requesting information related to the user who was assigned to the above IP address. According to the information received from "Midtel.net," Edward Werner was assigned the above IP address during the relevant time period and received Internet service at his residence from August 11, 1999 through to June 2015.

24. Among the information collected by the NIT when it was deployed against "cunnylicker" was the computer logon name "Eddie."

25. On December 15, 2015, I interviewed Edward Werner. During that interview he admitted to using the username "cunnylicker" to log into "Website A." He also admitted to viewing child pornography on "Website A" prior to the date of the interview.

26. On December 16, 2015, Edward Werner was questioned as part of a voluntary polygraph examination by Special Agent Alexander McDonald and Special Agent Brian

Seymour. During that examination, I observed Edward Werner again admit that he accessed "Website A" by using the username "cunnylicker." Edward Werner also stated that while being logged into "Website A", he accessed numerous threads and viewed numerous images and videos depicting minor children engaging in sexually explicit conduct with adults, including images and movies of female children ages six to eight engaged in oral sex with adult males. Edward Warner further stated that he had an interest in viewing images and movies of what he described as "preteen hardcore" pornography.


### III. CONCLUSION

27. Based on the foregoing, I believe there is probable cause to conclude that Edward Werner did knowingly receive and attempted to receive child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, that is, through accessing and viewing content on "Website A", in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1).



David C. Fallon  
Special Agent  
Federal Bureau of Investigation

Sworn to me this 16th day of December, 2015,



Hon. Christian F. Hummel  
United States Magistrate Judge